



**Digital Egypt Pioneers Initiative**



# Final Project

Implementing a Secure Multi-Branch Office  
Network

# Team Members

**Moahmed Nasser Mohamed Elshamy**

**Mohamed Moomen Abd El Hamid**

**Hazem Ahmed Saad Abdel Aziz**

**Imad Abdel Hamid Ali Attia**

**Moustafa Hossam Hassien**

**Mohamed Hosny Mohamed**

# Content

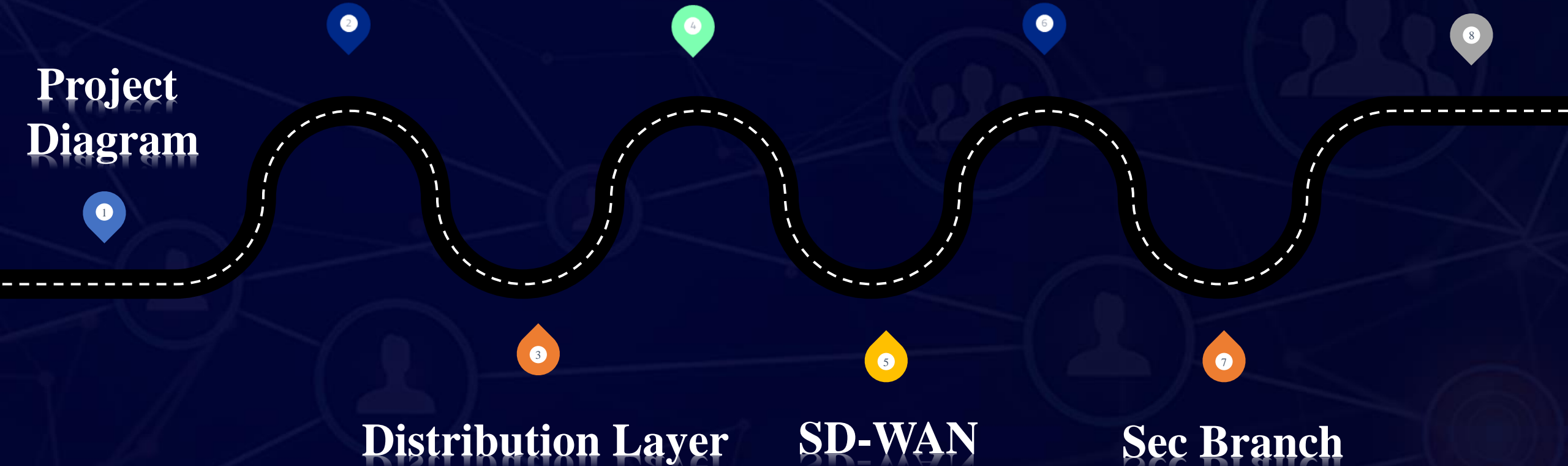
Access Layer

Firewall

VPN

Tests

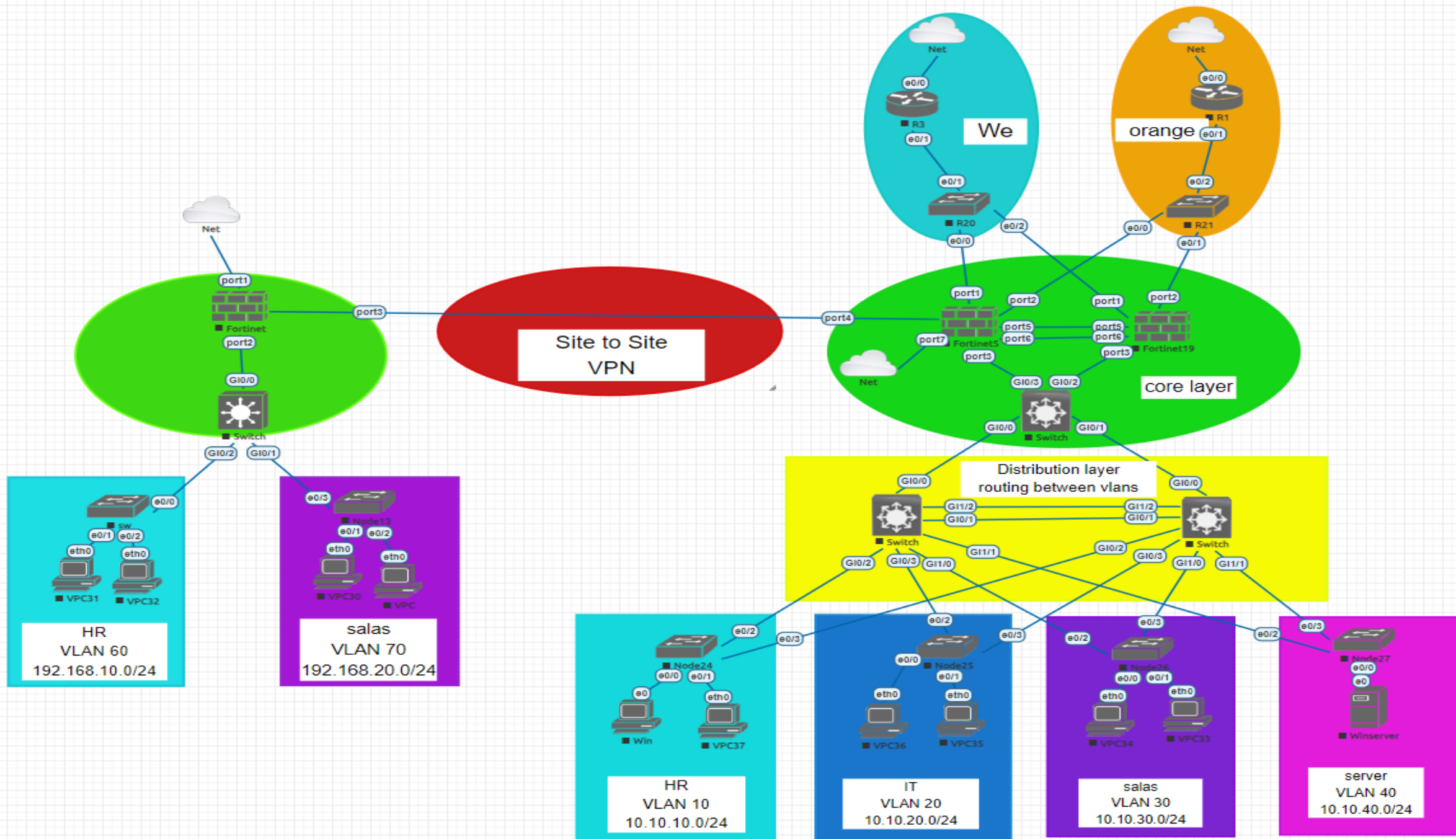
Project  
Diagram





1

# Project Diagram





2

Access layer

## ➤ Access Layer

- ❑ The access layer grants end devices access to the network. In the WAN environment, it may provide teleworkers or remote sites access to the corporate network across WAN connections.
- ❑ Generally incorporates Layer 2 switches and access points providing connectivity and serves a number of functions including:
  - Layer 2 switching
  - High availability
  - Port security
  - Address Resolution Protocol (ARP) inspection
  - Rapid PVST
  - Basic setting ( SSH - ACL for ssh )



## ➤ configuration

### ➤ All access switch

```
En
Conf t
Hostname access-sw
Username cisco password cisco
Enable password cisco
Banner motd & no unathorised access &
No ip domin-lookup
Service password-encryption
Line console 0
Password cisco
Login local
Exec-timeout 00
Logging synchronous
```

```
Exit
Ip domin-name cisco.com
Crypto key generate rsa general key modulus 1024
Ip ssh version 2
Line vty 0 15
Login local
Transport input ssh
Exit
Access-list 1 permit 192.168.30.0 0.0.0.255
Access-list 1 deny any
Line vty 0 15
Access-class 1 in
Exit
```



## ➤ configuration

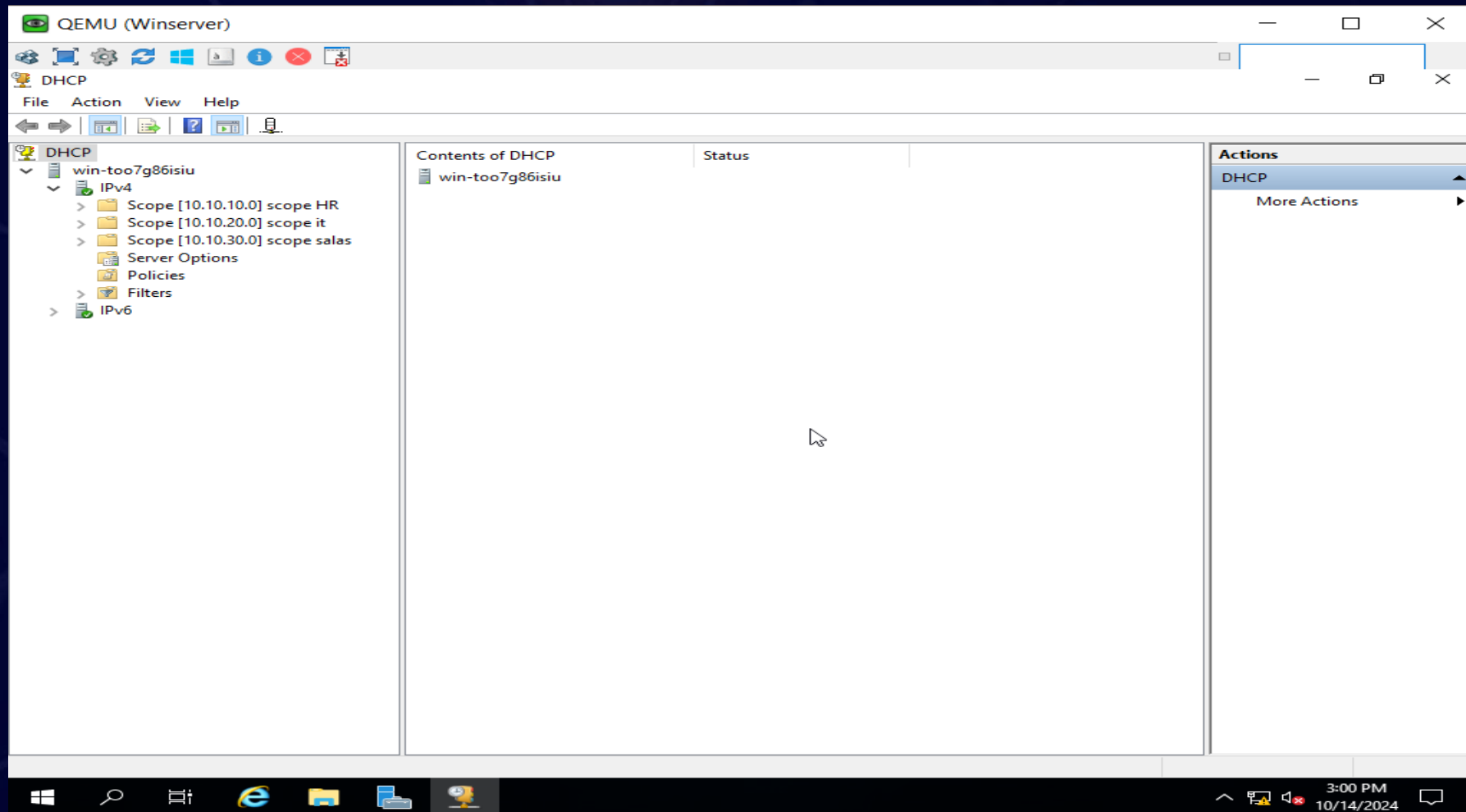
### ➤ All access switch

```
en
Conf t
Int range e0/2-3
Switchport trunk encapsulation dot1Q
Switchport mode trunk
Switchport nonegotiation
Exit
Vtp domain cisco.com
Vtp password 123
Vtp version 3
Vtp mode client
Do show vlan
Spanning-tree mode rapid-pvst
Spanning-tree vlan1,10,20,30,40
Ip dhcp snooping vlan 1,10,20,30,40
```

```
Int e0/0-1
Switchport mode access
Switchport access vlan 10
Spanning-tree portfast
Spanning-tree Bpdugard enable
Switchport portsecurity
Switchport portsecurity max 1
Switchport portsecurity mac-address stacky
Switchport portsecurity violation shutdown
Ip dhcp snooping l imit-rate 4
Int range e0/2-3
Ip dhcp snooping trust
Exit
Errdisable recovery interval 30
Errdisable recovery cuase portsecurity
```

# ➤ configuration

## ➤ Windows server (DHCP)

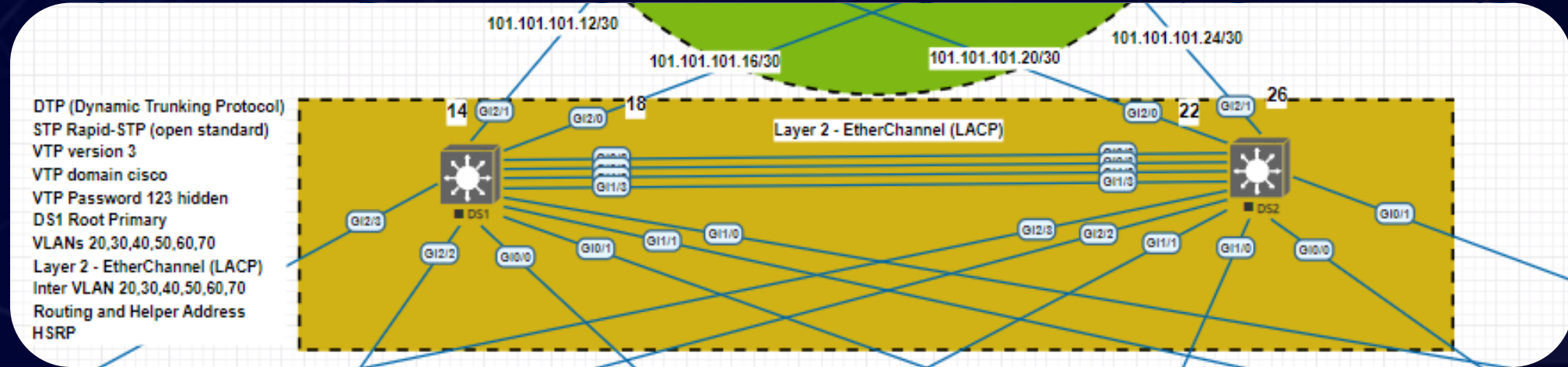




3

# Distribution Layer

## ➤ Distribution Layer



- The distribution layer is the boundary between the Layer 2 and the Layer 3 routed network.
- Layer 2 ether-channel.
- Routing services between LANs and VLANs and between routing domains.
- Redundancy.

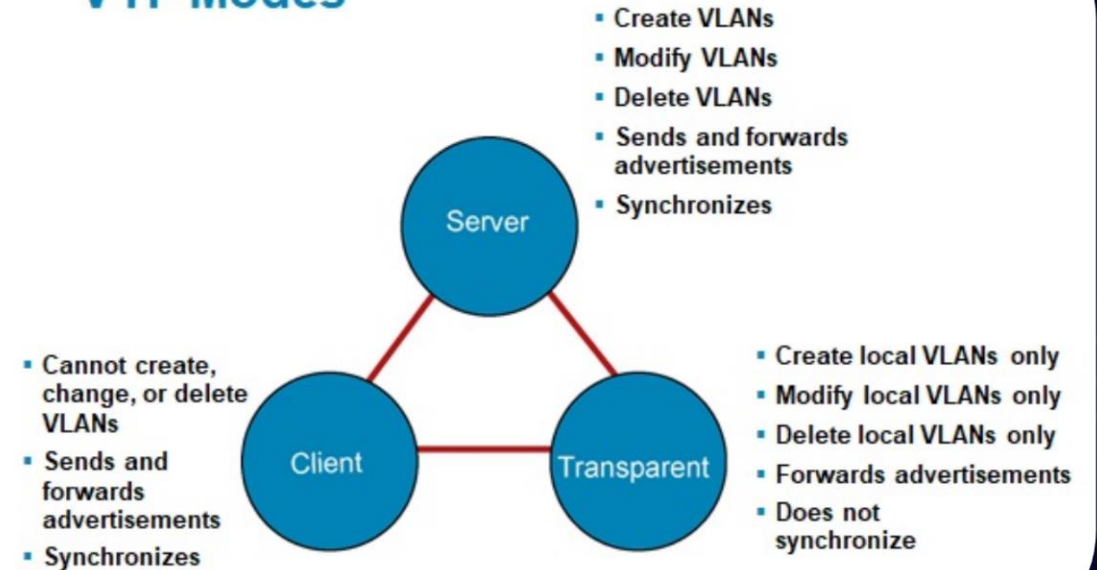
## ➤ Distribution Layer

### ➤ VTP (VLAN Trunking Protocol):

What's VTP ?

What's VTP V3?

#### VTP Modes



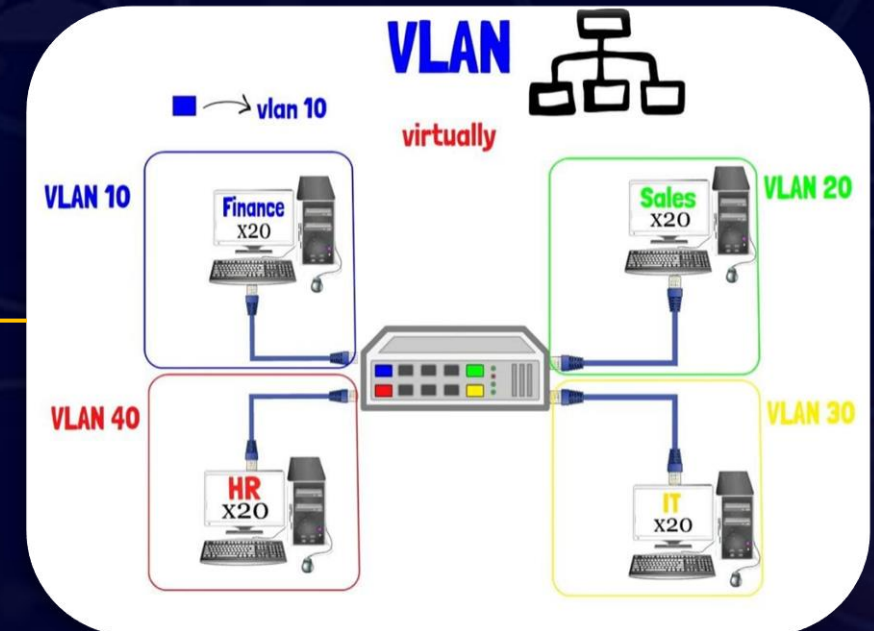
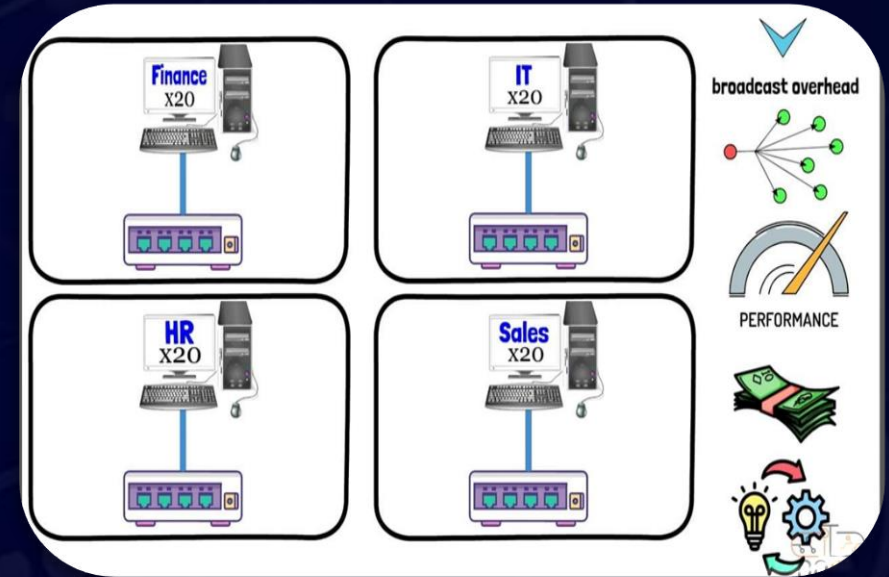


## ➤ VLANs (Virtual Local Area Network):

### What's VLAN?

#### ❑ Advantages of a VLAN:

- ❑ Separate broadcast domain.
- ❑ Decrease broadcast domain.
- ❑ Enhance network performance.
- ❑ Scalable.
- ❑ More security.





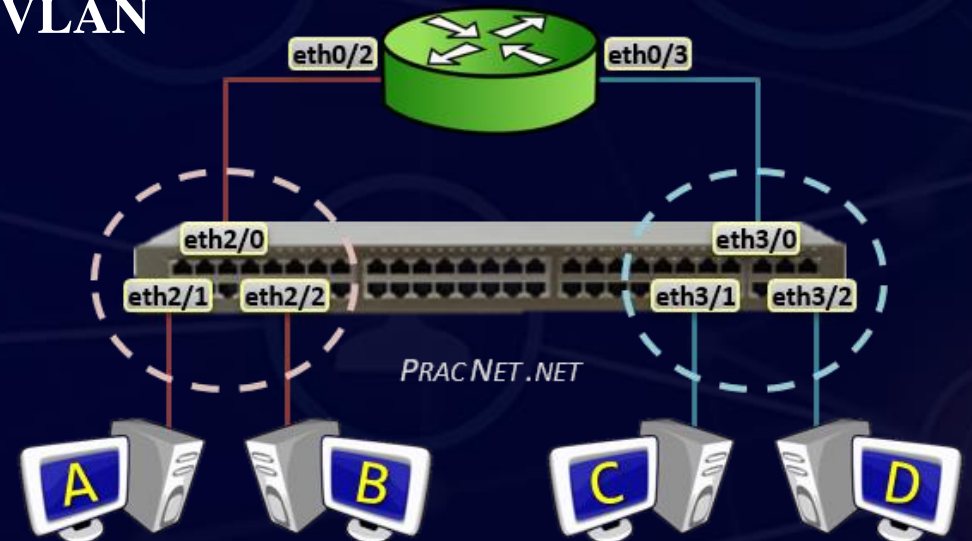
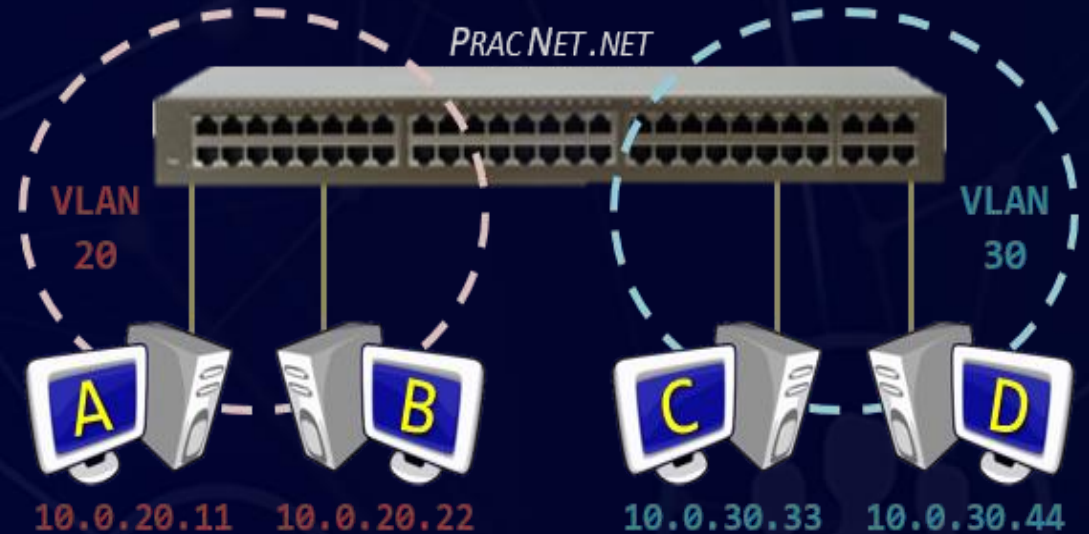
## ➤ Routing Between VLANs

### ➤ Why do we need Routing Between VLANs?

### ➤ There are three options available to enable routing between the VLANs:

- ✓ Router with a Separate Physical Interface in each VLAN
- ✓ Router with a Sub-Interface in each VLAN
- ✓ Using a Layer 3 Switch ( Best method )

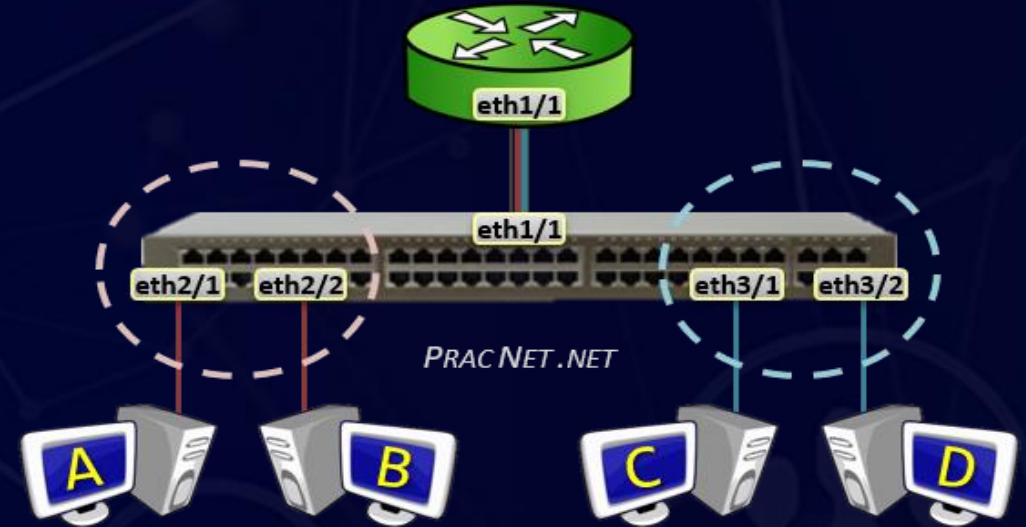
### ➤ Router with a Separate Physical Interface in each VLAN ( Traditional Method)



## ➤ Router with a Sub-Interface in each

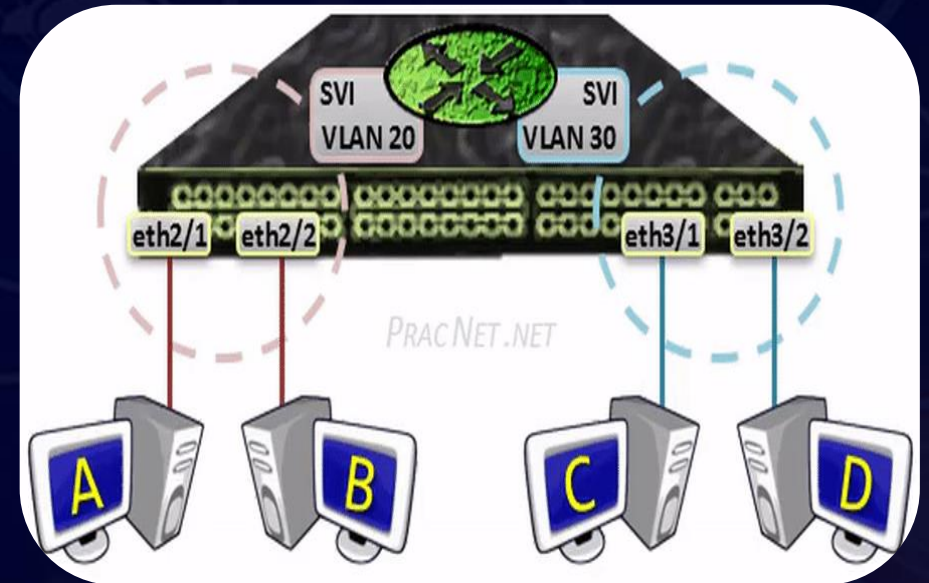
### VLAN ( Router on a Stick )

- A Sub-Interface allows a single Physical interface to be split up into multiple virtual sub-interfaces, each of which terminate their own VLAN.



## ➤ Layer 3 Switch ( Best method )

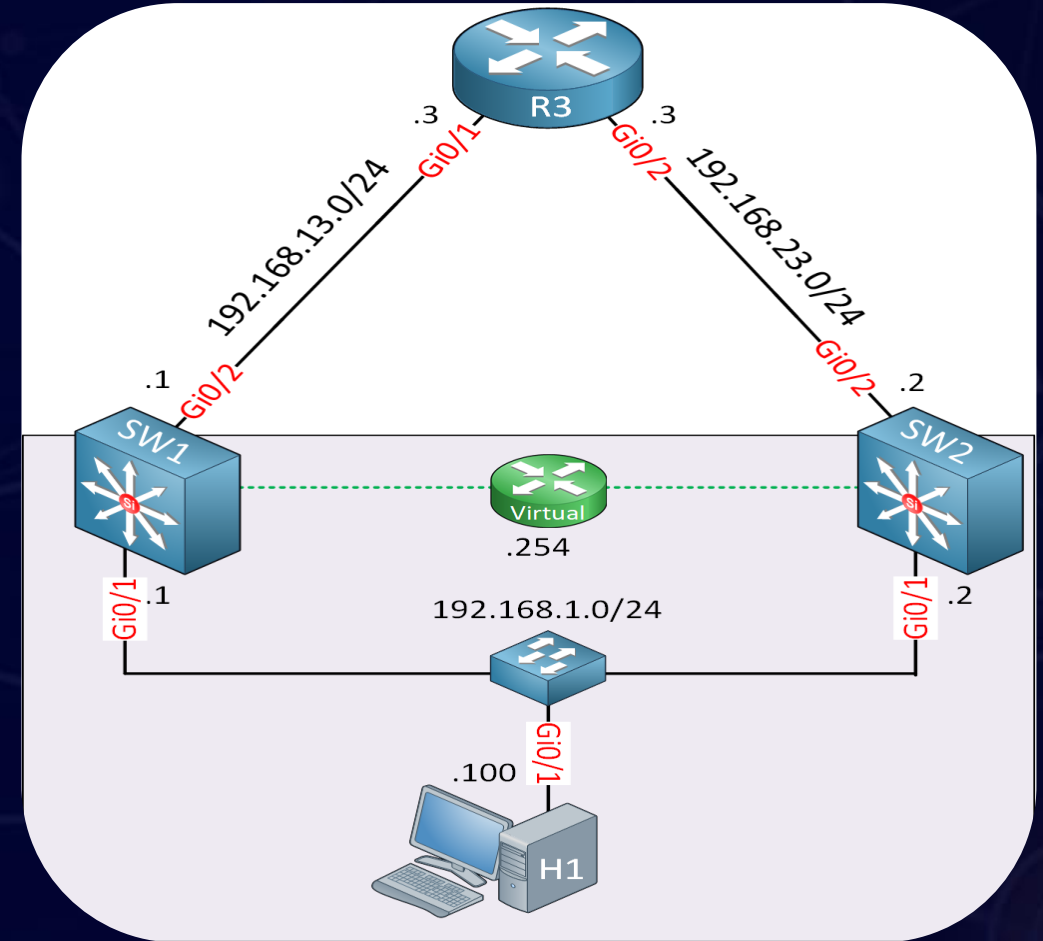
- You have the option of configuring an IP address within what is known as an SVI ( Switched Virtual Interface )
- The configuration for an SVI involves two parts. First, enabling IP Routing; and Second, applying an IP address to the VLAN.
- This IP will be the default gateway for the VLAN.



## ➤ VRRP

# What's VRRP?

- Active
- Standby
- Virtual gateway



## ➤ configuration

### ➤ Distribution switch

```
en
conf t
hostname core-sw2
username cisco password cisco
banner motd & no unathorised access &
enable password cisco
service password-en
no ip domain-lookup
line console 0
login local
exec-timeout 00
logging syn
exit
```

```
ip domain-name cisco.com
crypto key generate rsa general-keys modulus 1024
ip ssh version 2
line vty 0 15
transport input ssh
Exit
Access-list 1 permit 192.168.30.0 0.0.0.255
Access-list 1 deny any
Line vty 0 15
Access-class 1 in
Exit
```



## ➤ configuration

### ➤ Distribution switch

```
en
conf t
vtp domain cisco.com
vtp password 123
vtp version 3

vlan 10
name HR
vlan 20
name it
vlan 30
name salas
vlan 40
name server
Exit
spanning-tree mode rapid-pvst
```

```
spanning-tree vlan 1,10,20,30,40 priority 24576
```

```
interface GigabitEthernet0/0
no switchport
ip address 10.10.50.2 255.255.255.0
negotiation auto
vrrp 50 ip 10.10.50.4
vrrp 50 priority 150
vrrp 50 authentication text cisco
vrrp 50 track 1 decrement 60
```

```
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
negotiation auto
```

## ➤ configuration

### ➤ Distribution switch

```
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
negotiation auto
```

!

```
interface GigabitEthernet0/2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
negotiation auto
```

!

```
interface GigabitEthernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
negotiation auto
```

```
interface GigabitEthernet1/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
negotiation auto
```

!

```
interface GigabitEthernet1/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
negotiation auto
```

!

```
interface GigabitEthernet1/2
no switchport
ip address 10.10.60.1 255.255.255.0
negotiation auto
```

!



## ➤ configuration

### ➤ Distribution swihch

```
interface Vlan10
ip address 10.10.10.2 255.255.255.0
ip helper-address 10.10.40.4
vrrp 10 ip 10.10.10.1
vrrp 10 priority 150
vrrp 10 authentication text cisco
vrrp 10 track 1 decrement 60
```

!

```
interface Vlan20
ip address 10.10.20.2 255.255.255.0
ip helper-address 10.10.40.4
vrrp 20 ip 10.10.20.1
vrrp 20 priority 150
vrrp 20 authentication text cisco
vrrp 20 track 1 decrement 60
```

!

```
interface Vlan30
ip address 10.10.30.2 255.255.255.0
ip helper-address 10.10.40.4
vrrp 30 ip 10.10.30.1
vrrp 30 priority 150
vrrp 30 authentication text cisco
vrrp 30 track 1 decrement 60
```

!

```
interface Vlan40
ip address 10.10.40.2 255.255.255.0
vrrp 40 ip 10.10.40.1
vrrp 40 priority 150
vrrp 40 authentication text cisco
vrrp 40 track 1 decrement 60
```

!

```
ip route 0.0.0.0 0.0.0.0 10.10.50.1
```

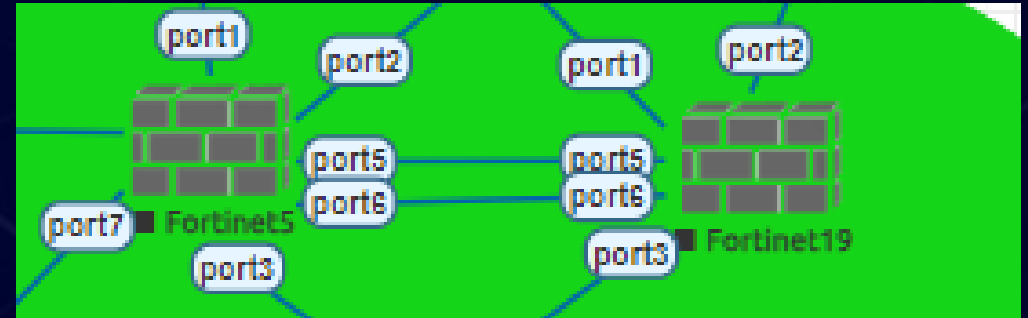


4

# Firewall

# ➤ Firewall

- A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules
- Its primary function is to establish a barrier between trusted internal networks and untrusted external networks, such as the internet, to prevent unauthorized access and potential threats.



# ➤ Firewall

## ➤ High Availability (HA)

- ❑ High Availability (HA) in FortiGate firewalls provides redundancy by using multiple devices. If one fails, another takes over to ensure continuous service without downtime.

FortiGate VM64-KVM

1 3 5 7 9 11 13 15 17 19 21 23

2 4 6 8 10 12 14 16 18 20 22 24

FGT-master (Primary)

Refresh

Edit

Remove device from HA cluster

Status	Priority	Hostname	Serial No.	Role	System Uptime	Sessions	Throughput
✓ Synchronized	150	FGT-master	FGVMEVBVMKSKUG31	Primary	23m 41s	0	65.00 kbps

# ➤ Firewall

## ➤ Interface ( WAN PORT)


	 vpn (port4)	 Physical Interface	192.168.201.1/255.255.255.0	PING
	 WAN Orange (port1)	 Physical Interface	<u>200.20.20.1/255.255.255.0</u>	PING HTTPS SSH <b>HTTP</b> FMG-Access
	 WAN We (port2)	 Physical Interface	100.10.10.2/255.255.255.0	PING HTTPS SSH FMG-Access

# ➤ Firewall

## ➤ Interface ( LAN PORT )

Edit Interface


Name


 lan (port3)

Alias


lan

Type

 Physical Interface

VRF ID 

0

Role 

LAN

Address

Addressing mode

Manual

DHCP

Auto-managed by IPAM

IP/Netmask

10.10.50.1/255.255.255.0

Create address object matching subnet

☐

Secondary IP address

☐

Administrative Access

IPv4


☐ HTTPS

☐ SSH

☐ RADIUS Accounting

☒ PING


☐ SNMP

☐ Security Fabric Connection 

☐ FMG-Access

☐ FTM


☐ Speed Test

Receive LLDP 

Use VDOM Setting

Enable

Disable

Transmit LLDP 

Use VDOM Setting

Enable

Disable

☐ DHCP Server



# ➤ Firewall

## ➤ Security profile (IPS)

- ❑ The IPS (Intrusion Prevention System) in FortiGate inspects network traffic for malicious activity and potential threats, such as intrusion attempts or vulnerability exploits. It automatically blocks or alerts on detected threats to protect the network in real time.

The screenshot shows the FortiGate IPS configuration interface. The 'Filter' tab is active, displaying a list of protocols and OSes. The 'Signature' tab is also visible. The main table lists IPS signatures with columns for Name, Severity, Target, and OS. The 'OS' column is expanded, showing a search bar and a list of operating systems and applications.

Name	Severity	Target	OS
IPS Signature 1,475			
AOL.Radio.ActiveX.Remote.Stack.Overflow	Severity 5 (5 red squares)	Client	Windows
AVS.Media.Player.ActiveX.setsource.Method...	Severity 5 (5 red squares)	Client	Windows
AXIS.Communications.Camera.Control.Buffer...	Severity 5 (5 red squares)	Client	Windows

The 'OS' column is expanded, showing a search bar and a list of operating systems and applications:

- PROT SNMP
- PROT SSH
- PROT SSL
- PROT TCP
- PROT TELNET
- PROT TFN
- PROT UDP
- OS (6)
- OS BSD
- OS Linux
- OS MacOS
- OS Other
- OS Solaris
- OS Windows
- APPLICATION (36)
- APP Adobe
- APP Apache
- APP Apple
- APP ASP\_app
- APP CA
- APP CGI\_app
- APP Cisco

## ➤ Firewall

### ➤ Security profile (antivirus)

- ❑ The antivirus feature in FortiGate scans network traffic and files for viruses, malware, and other malicious content. It prevents infections by detecting and blocking harmful files before they can reach devices on the network.

Edit AntiVirus Profile

Name: test

Comments: Scan files and block viruses. 29/255

AntiVirus scan: ☒ **Block** Monitor

Feature set: **Flow-based** Proxy-based

Inspected Protocols

- HTTP ☒
- SMTP ☒
- POP3 ☒
- IMAP ☒
- FTP ☒
- CIFS ☒

APT Protection Options

- Treat Windows executables in email attachments as viruses ☒
- Include mobile malware protection ☒
- Quarantine ☒

Virus Outbreak Prevention ⓘ

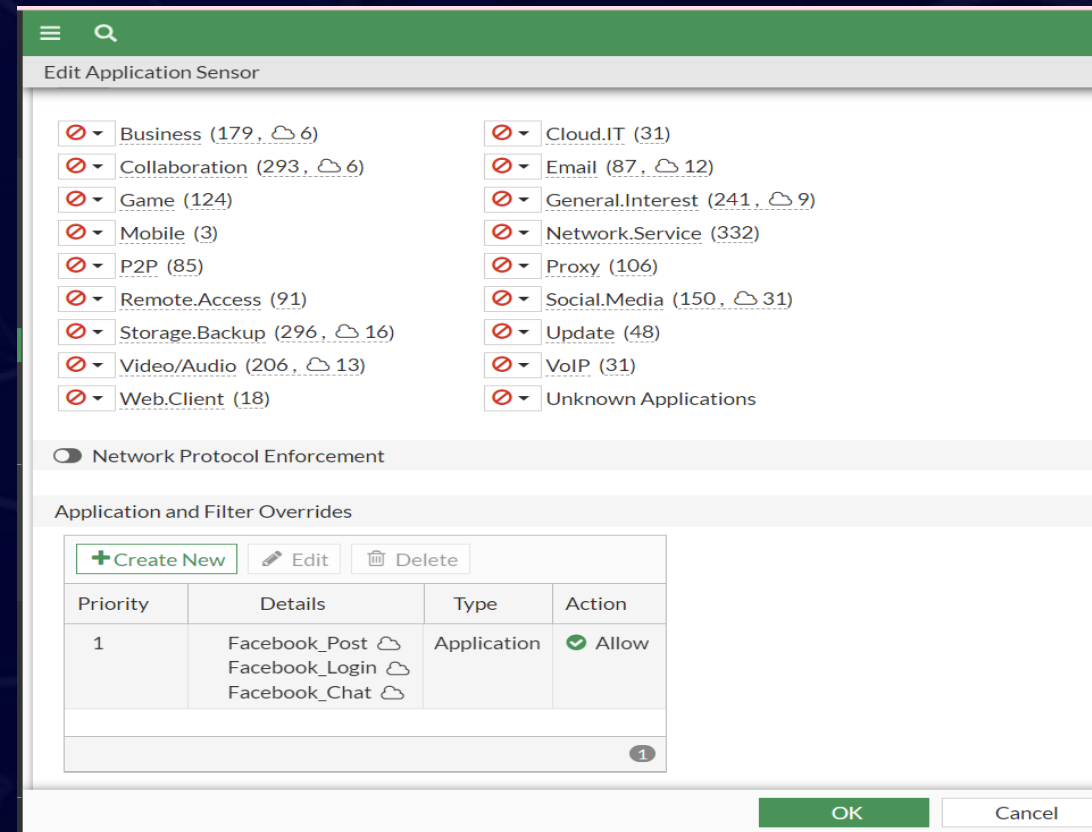
Use FortiGuard outbreak prevention database ☐

OK Cancel

# ➤ Firewall

## ➤ Security profile (web filter)

- ❑ The web filtering feature in FortiGate controls access to websites by categorizing and blocking harmful or inappropriate content. It helps enforce security policies and protect users from malicious sites, phishing, and other online threats.



# ➤ Firewall

## ➤ Security profile (file filter)

- ❑ The file filter feature in FortiGate blocks or restricts access to specific file types within network traffic. It helps prevent the transfer of unauthorized or malicious files, enhancing data security and compliance.

Create New File Filter Rule

Name: test

Comments: Write a comment... 0/255

Protocols: CIFS, FTP, HTTP, IMAP, POP3, SMTP

Traffic: Incoming, Outgoing, Both

Match Files

Password-protected only: ☐

File types: html, pdf, zip

Action: ☒ Monitor, ☐ Block

Select Entries

Search:

.net, 7z, activemime, arj, aspack, avi, base64, bat, binhex, bmp, bzip, bzip2, cab, chm, class, cod, crx, dmg, elf, exe, flac, fsg, gif

OK, Cancel, Close

# ➤ Firewall

## ➤ Security profile (In policy )

Edit Policy

Inspection Mode

Flow-based

Proxy-based

Firewall / Network Options

NAT

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Preserve Source Port

Passive Health Check

Protocol Options

PROT

default

Security Profiles

AntiVirus

AV

test

Web Filter

WEB

test

DNS Filter

Application Control

APP

test

IPS

IPS

test

File Filter

FF

test

SSL Inspection













SSL

certificate-inspection

# ➤ Firewall

## ➤ Internet policy

Edit Policy

Name 	internet	
Incoming Interface	 lan (port3) 	
	+	
Outgoing Interface	 SD-WAN ZONE 	
	+	
Source	 all 	
	+	
Destination	 all 	
	+	
Schedule	 always ▼	
Service	 ALL 	
	+	
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY	
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based	

Firewall / Network Options

NAT ☒

IP Pool Configuration ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

Preserve Source Port ☐

Passive Health Check ☐

OK Cancel



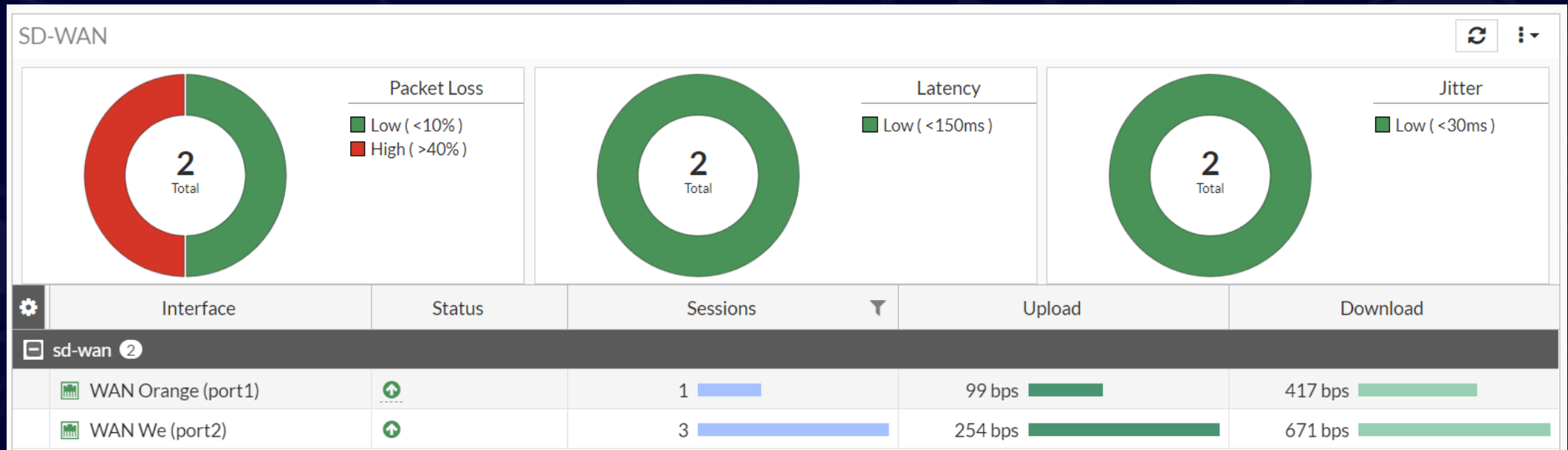


5

SD-WAN

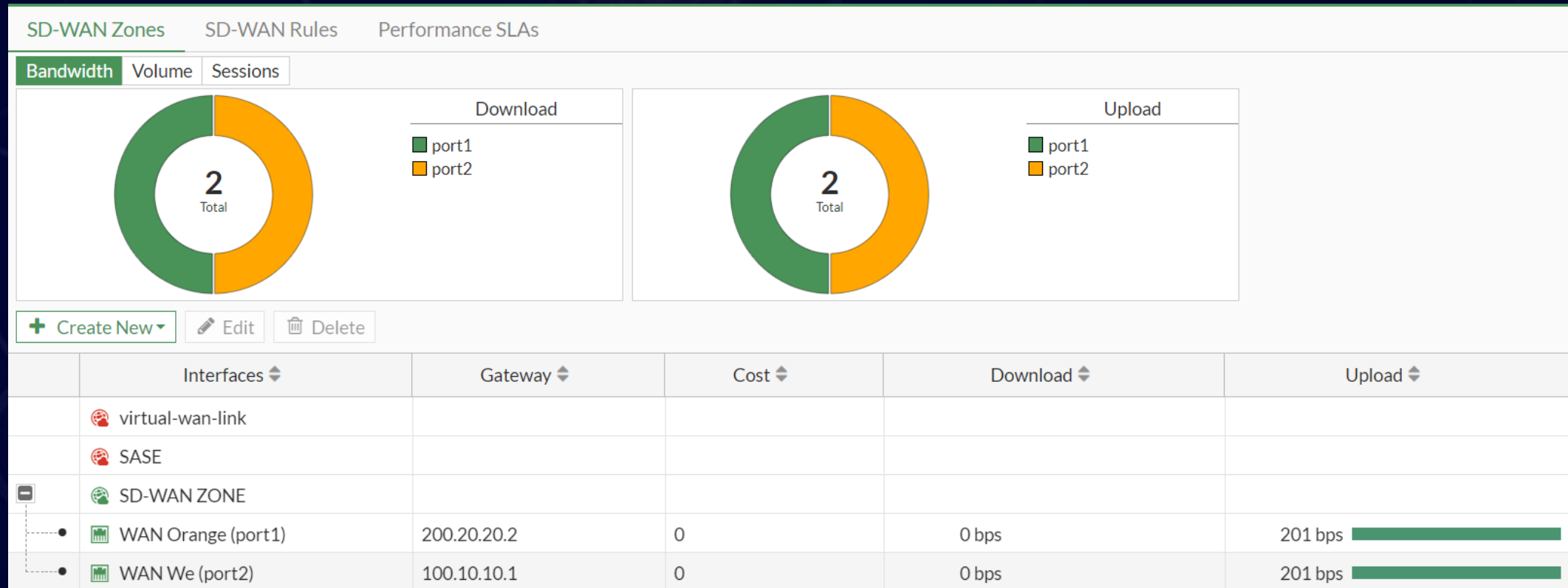
# ➤ SD-WAN

- ❑ The SD-WAN feature in FortiGate optimizes and manages multiple WAN connections, improving performance and reliability. It intelligently routes traffic based on application needs, ensuring secure and efficient connectivity across different network paths.



# ➤ SD-WAN

## ➤ Sd-wan zone




# ➤ SD-WAN

## ➤ Sd-wan LSA

Edit Performance SLA

Name

sdwan

Probe mode 

Active

Passive

Prefer Passive

Protocol


Ping

HTTP

DNS

Server



8.8.8.8




Participants

All SD-WAN Members


Specify

SLA Target  

Latency threshold 


500

ms

Jitter threshold 

500

ms

Packet Loss threshold 

50


%

Link Status


Check interval

5000

ms

Failures before inactive 



5

Restore link after 

5

check(s)


Actions when Inactive

Update static route  

# ➤ SD-WAN

## ➤ Sd-wan Role

Priority Rule

Application 

+

Outgoing Interfaces

Select a strategy for how outgoing interfaces will be chosen.

☐ Manual

Manually assign outgoing interfaces.

☐ Best Quality

The interface with the best measured performance is selected.

☒ Lowest Cost (SLA)

The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.


☐ Maximize Bandwidth (SLA)

Traffic is load balanced among interfaces that meet SLA targets.

Interface preference

+

Zone preference

 SD-WAN ZONE

+

×

Required SLA target

sdwan

+

×


Forward DSCP


☐

Reverse DSCP

☐

Status

 Enable

 Disable



6

VPN



# ➤ VPN

## ➤ Site to site vpn

- ❑ The site-to-site VPN in FortiGate establishes secure, encrypted tunnels between different networks over the internet. It enables seamless communication between remote sites, ensuring data confidentiality and integrity while allowing centralized management and access control.

IPsec							
<div>Reset Statistics Bring Up Bring Down Locate on VPN Map</div>							
Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors	Comments
Site to Site - FortiGate 1							
ipsec	192.168.201.2		544 B	420 B	ipsec	ipsec	VPN: ipsec (Created by VPN wi



7

Tests

# ➤ Test

## ➤ Test routing between vlan

```
VPC36

Welcome to Virtual PC Simulator, version 1.0 (0.8c)
Dedicated to Daling.
Build time: Dec 31 2016 01:22:17
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

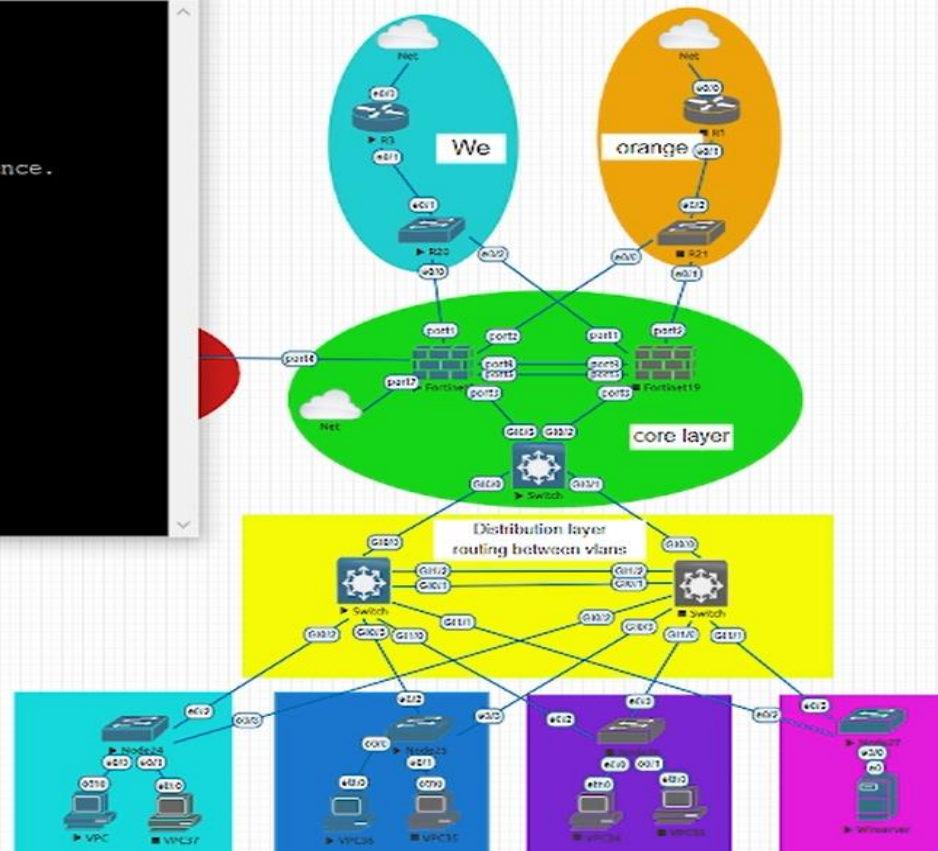
VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Modified version supporting unetlab by unetlab team

Press '?' to get help.

VPCS> ip dhcp
DORA IP 10.10.20.5/24 GW 10.10.20.1

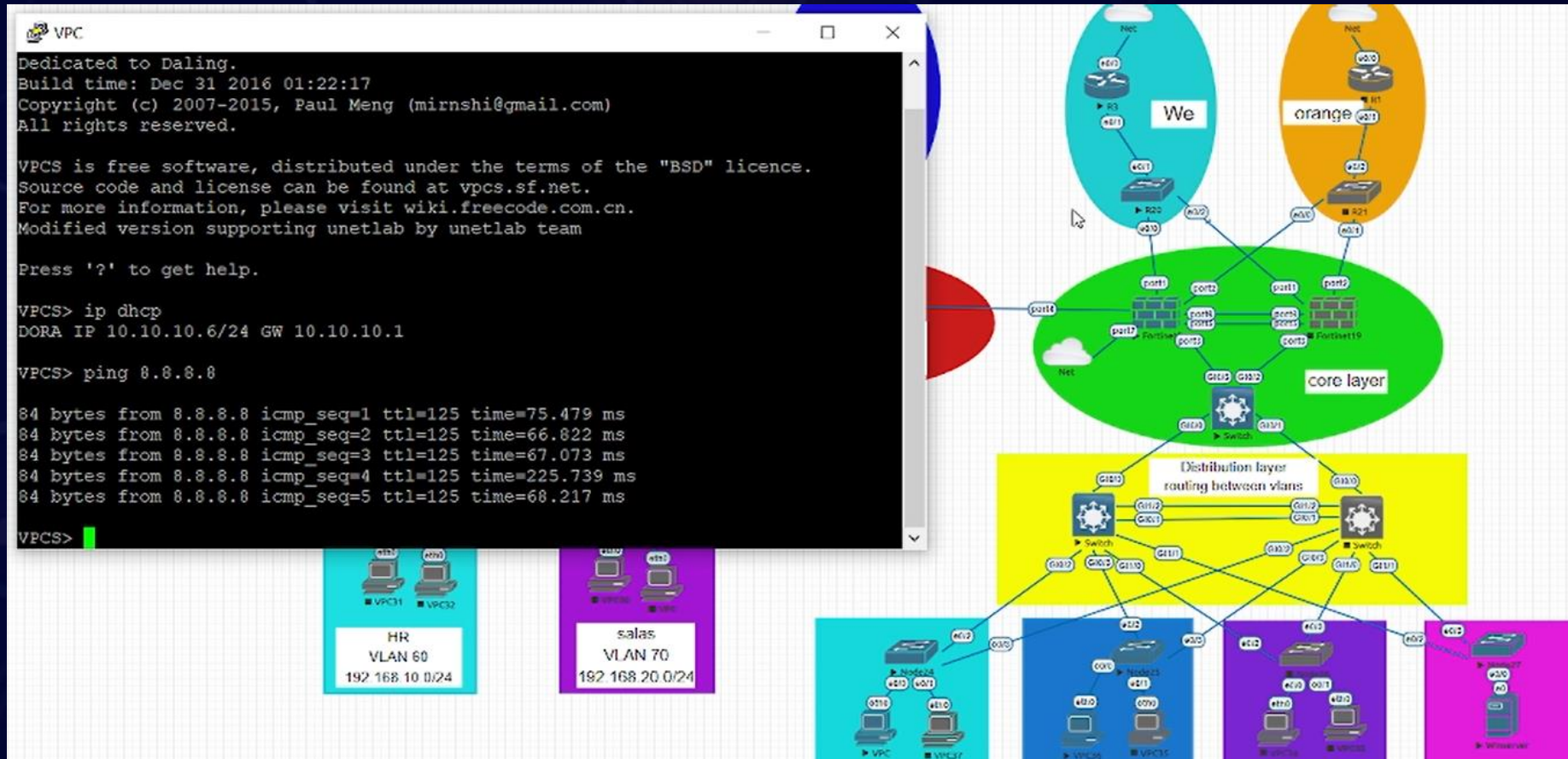
VPCS> ping 10.10.10.6

84 bytes from 10.10.10.6 icmp_seq=1 ttl=63 time=9.439 ms
84 bytes from 10.10.10.6 icmp_seq=2 ttl=63 time=4.365 ms
84 bytes from 10.10.10.6 icmp_seq=3 ttl=63 time=4.084 ms
```



# ➤ Test

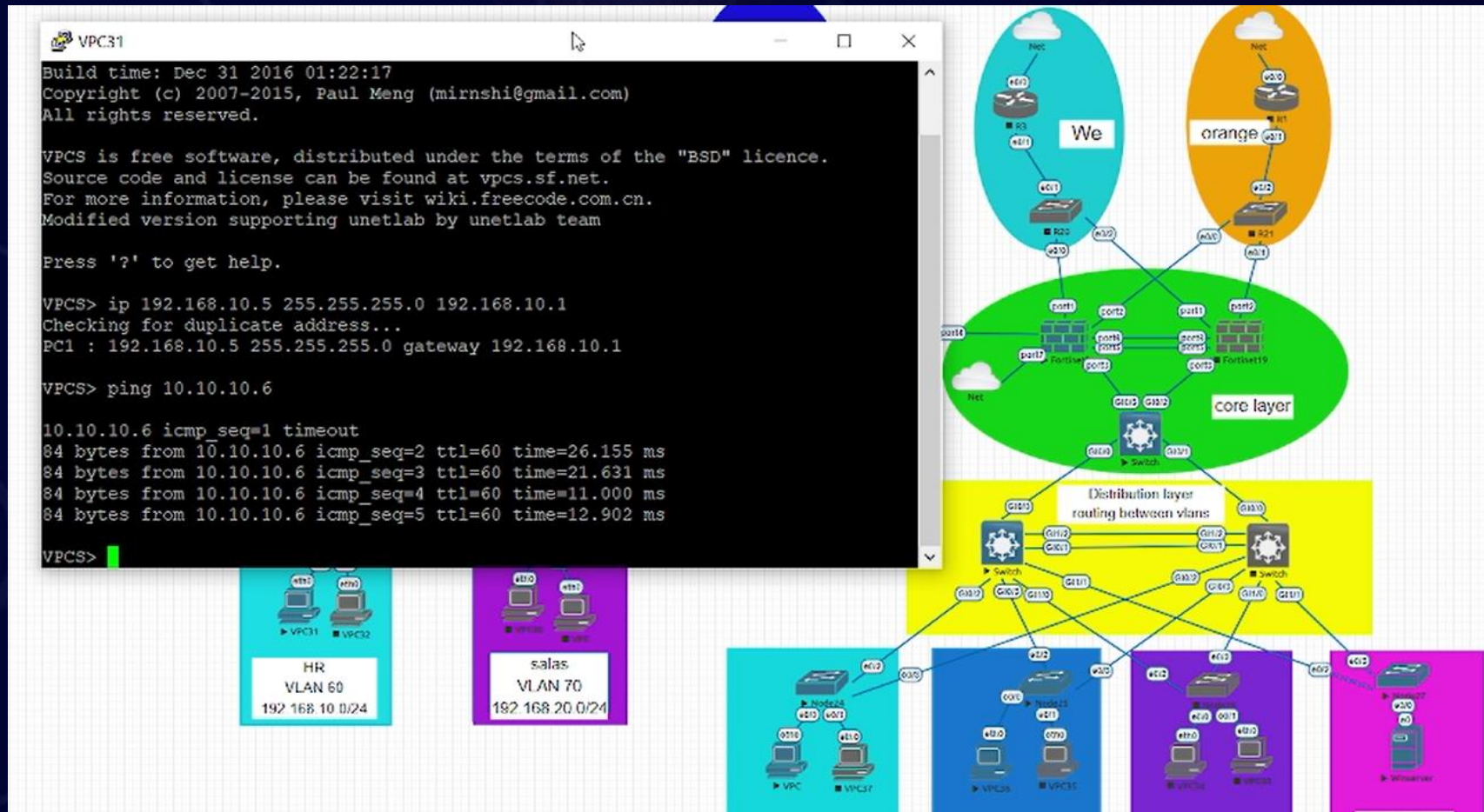
## ➤ Test internet





## ➤ Test

## ➤ Test connectivity between two sites





*Thank You*

*For your time*